

08 - 06 - 08

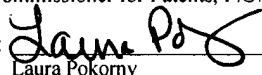
15W AS-



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application No. : 10/748,489
Applicants : Timothy C. Loose
Filed : December 30, 2003
Title : Gaming Machine Having Sampled Software Verification
TC/A.U. : 2137
Examiner : Jeffrey D. Popham
Docket No. : 247079-00243USPT
Customer No. : 70243

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

<u>CERTIFICATE OF MAILING 37 C.F.R. 1.10</u>	
EXPRESS MAIL NO.:	EM 143187892 US
DATE OF DEPOSIT:	August 5, 2008
I hereby certify that this paper or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.	
Signature:	 Laura Pokorny

APPEAL BRIEF PURSUANT TO 37 C.F.R. § 41.37

Dear Commissioner:

This Appeal Brief is filed pursuant to the Appellants' appeal to the Board of Patent Appeals and Interferences ("Board") from the final rejection of claims 1-23 in the February 28, 2008 Final Office Action. (Exhibit B). A Notice of Appeal was filed on June 5, 2008. (Exhibit C).

The due date for this Appeal Brief is two months from the mailing date of the Notice of Appeal (*i.e.*, August 5, 2008).

I. REAL PARTY IN INTEREST

The real party in interest is WMS Gaming Inc., having a place of business at 800 South Northpoint Boulevard, Waukegan, IL 60085.

08/06/2008 MGE BRE#1 00000064 10748489
01 FC:1402 510.00 OP

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board of Patent Appeals and Interferences in the present appeal.

III. STATUS OF CLAIMS

Claims 1-23 are currently pending and rejected in the above-referenced application and are the subject of the present appeal. No claims have been allowed.

IV. STATUS OF AMENDMENTS

The claims are as currently listed in a May 8, 2008 amendment and response to Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1-23 are directed to the embodiments shown in Figs. 1, 2 and 4-6. Independent claim 1 is generally directed to a method of authenticating a media device (46, 48, 50) in a gaming machine 10. *See* U.S. Publ. No. U.S. Publication No. 2005/0143171¹ (Exhibit A, ¶¶ 8, 17 and 59, Specification, p. 5, ll. 3-5, p. 6, ll. 15-17, p. 27, ll. 5-7, Figs. 1-2). An address pointer ADDR is set to a first next memory location in the media device. (Exhibit A, ¶ 61, Specification, p. 27, ll. 15-17, Fig. 4). It is determined whether the first next memory location is a last memory location to be authenticated in the media device. (Exhibit A, ¶ 62, Specification, p. 28, ll. 3-4, Fig. 4). A hashing algorithm is applied to contents of the first next memory location and a key-

¹ The Publication for the application at issue is being attached for convenience as Exhibit A. Applicant is also providing the corresponding specification page and line number in this and following sections.

value is updated. (Exhibit A, ¶ 62, Specification, p. 28, ll. 7-10, Fig. 4). A predetermined number N is added to ADDR such that a next ADDR=ADDR+N, wherein N is equal to a positive or negative integer excluding -1, 0 and 1. (Ex. A, ¶¶ 62 and 65, Specification, p. 28, ll. 4-7, p. 29, ll. 8-11, Fig. 4). The next ADDR is set to a next memory location in the media device to be authenticated such that the next memory location is separated from the first next memory location by at least one memory location. (Exhibit A, ¶ 62, Specification, p. 28, ll. 7-10, Fig. 4). The determining, applying, adding and setting steps are repeated until the next ADDR is equal to the last memory location. (Ex. A, ¶ 62, Specification, p. 28, ll. 10-13, Fig. 4). It is determined whether the key-value is equal to a predetermined key. (Ex. A, ¶ 63, Specification, p. 28, ll. 16-18, Fig. 4). In response to the key-value being equal to the predetermined key, authentication is passed. (Ex. A, ¶ 63, Specification, p. 28, ll. 18-19, Fig. 4). In response to the key-value not being equal to the predetermined key, authentication is failed. (Ex. A, ¶ 63, Specification, p. 28, l. 19 to p. 29, l. 2, Fig. 4).

Claim 13 generally relates to a gaming machine 10 including a user interface 16. (Ex. A, ¶¶ 18, 19 and 21, Specification, p. 7, ll. 4-18, p. 9, ll. 9-12, Figs. 1-2). A central processing unit (CPU) 30 is coupled to the user interface 16. (Ex. A, ¶ 20, Specification, p. 7, l. 19 to p. 8, l. 3, Fig. 2). The CPU 30 includes a processor 32. (Ex. A, ¶ 21, Specification, p. 8, l. 9, Fig. 2). A first memory 36 is coupled to the processor 32, the first memory is adaptable to store data in a plurality of memory locations. (Ex. A, ¶ 20, Specification, p. 8, ll. 11-12, Fig. 2). A second memory 48 is coupled to the processor 32. (Ex. A, ¶ 22, Specification, p. 9, ll. 3-14, Fig. 2). The second memory 48 is adapted to contain executable program code. (Ex. A, ¶ 26, Specification, p. 11, ll. 6-11). The executable program code further includes a plurality of instructions configured to cause the processor 32 to determine the authenticity of the data in the

plurality of memory locations. (Ex. A, ¶ 26, Specification, p. 11, ll. 4-14). The instructions include instructions for performing a hash calculation on a sample of memory locations from the plurality of memory locations and calculating a key-value from the sample of memory locations. (Ex. A, ¶ 62, Specification, p. 28, ll. 4-13, Fig. 4). The sample of memory locations is a number of memory locations that is less than the plurality of memory locations and each memory location of the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory location. (Ex. A, ¶ 62, Specification, p. 28, ll. 4-13, Fig. 4). The key-value is compared to a predetermined key and the data stored in the plurality of memory locations is authenticated if the key-value is equal to the predetermined key. (Ex. A, ¶ 63, Specification, p. 28, ll. 16-19, Fig. 4). The data stored in the plurality of memory locations is not authenticated if the key-value is not equal to the predetermined key. (Ex. A, ¶ 63, Specification, p. 28, l. 19 to p. 29, l. 2, Fig. 4).

Claim 17 generally relates to a method of repeatedly authenticating a portion of a media device 48 in a gaming machine 10 that is turned on. (Ex. A, ¶¶ 17, 31, Specification, p. 6, ll. 15-17, p. 13, ll. 10-14, Figs. 1 and 4). A plurality of memory locations are read that are spaced from each other in the media device 48, such that each of the plurality of memory locations that is read is separated from the other memory locations by at least one memory location. (Exhibit A, ¶ 62, Specification, p. 28, ll. 4-13, Fig. 4). The plurality of memory locations is less than a total number of memory locations in the media device. (Ex. A, ¶ 62, Specification, p. 28, ll. 4-13, Fig. 4). After reading each memory location, a hash value is calculated, and the hash value is used to update a key-value until all of the plurality of memory locations are read and a final key-value is determined. (Ex. A, ¶ 63, Specification, p. 28, ll. 16-18, Fig. 4). The final key-value is compared to a predetermined key and the portion of the media device is passed as authentic if the

final key-value is equal to the predetermined key. (Ex. A, ¶ 63, Specification, p. 28, ll. 18-19, Fig. 4). The reading, calculating and comparing steps are repeated. (Ex. A, ¶ 62, Specification, p. 28, ll. 10-13, Fig. 4). The predetermined portion of the media device is not passed as authentic if the final key-value is not equal to the predetermined key, halting operation of the gaming machine 10. (Exhibit A, ¶ 63, Specification, p. 28, l. 19 to p. 29, l. 2, Fig. 4).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Whether claims 1-7, 11-14, 16-19 and 22-23 were improperly rejected as obvious under 35 U.S.C. § 103(a) over U.S. Patent Publication No. 2002/0049909 (“Jackson” attached as Exhibit D) in combination with U.S. Patent No. 5,644,704 (“Pease” attached as Exhibit E) and U.S. Patent No. 7,149,801 (“Burrows” attached as Exhibit F).

Claims 1-7, 11-14, 16-19 and 22-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson in view of Pease and Burrows. (Final Office Action, Ex. B, pp. 2-3). With respect to independent claim 1, the Final Office Action asserts that Jackson discloses a method of authenticating a media device in a gaming machine by applying a hashing algorithm to the contents of a first next memory location and updating a key value. (Ex. B, pp. 2-3). The Final Office Action asserts that Jackson discloses repeating the steps until the last memory location and determining whether the key value is equal to a predetermined key value to determine whether authentication is passed. (Ex. B, p. 3). The Final Office Action concedes that Jackson fails to disclose an address pointer ADDR which is set to the next memory location and adding a predetermined number N is added to ADDR such that a next ADDR=ADDR+N. (Ex. B, pp. 3-4). The Final Office Action asserts that Pease discloses memory locations which set an address point ADDR and setting the next ADDR as ADDR +N. (Ex. B, p. 4). The Final

Office Action asserts that it would be obvious to one of ordinary skill to incorporate the data addressing and verification system of Pease to the secure gaming system of Jackson to allow authentication of the memory to provide better verification/authentication of memory. (Ex. B, p. 4). The Final Office Action indicates that Burrows discloses that N is equal to a positive or negative integer excluding -1, 0 and 1. (Ex. B, p. 4). The Final Office Action asserts that it would have been obvious to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease.

With respect to independent claim 13, the Final Office Action asserts that Jackson discloses a gaming machine with a user interface, a CPU with a processor and a first and second memory coupled to the processor. (Ex. B, p. 7). The Final Office Action asserts that Jackson discloses storing a plurality of instructions to determine authenticity of data in the memory and repeating the steps until the last memory location and determining whether the key value is equal to a predetermined key value to determine whether authentication is passed. (Ex. B, p. 8). The Final Office Action concedes that Jackson fails to disclose that the hash calculation is performed on a sample of memory location that is less than the plurality of memory locations. (Ex. B, p. 8). The Final Office Action asserts that it would be obvious to one of ordinary skill to incorporate the data addressing and verification system of Pease to the secure gaming system of Jackson to allow authentication of the memory to provide better verification/authentication of memory. (Ex. B, p. 8). The Final Office Action indicates that Burrows discloses that the sample of memory locations are a number of memory locations that is less than all of the memory locations. (Ex. B, p. 9). The Final Office Action asserts that it would have been obvious to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks. (Ex. B, p. 9).

With respect to independent claim 17, the Final Office Action asserts that Jackson discloses a gaming machine that repeatedly authenticates a portion of a media device that reads a plurality of memory locations and calculates a hash value to update a key value. (Ex. B, p. 10). The Final Office Action asserts that Jackson discloses determining whether the key value is equal to a predetermined key value to determine whether authentication is passed. (Ex. B, p. 10). The Final Office Action concedes that Jackson fails to disclose memory locations in the form of addresses so each of the memory locations is separated by at least one memory location and the plurality of memory locations are less than the total number of memory locations in the media device. (Ex. B, pp. 10-11). The Final Office Action asserts that it would be obvious to one of ordinary skill to incorporate the data addressing and verification system of Pease to the secure gaming system of Jackson to allow authentication of the memory to provide better verification/authentication of memory. (Ex. B, p. 11). The Final Office Action indicates that Burrows discloses that the sample of memory locations is a number of memory locations that is less than all of the memory locations. (Ex. B, p. 11). The Final Office Action asserts that it would have been obvious to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks. (Ex. B, p. 11).

VII. ARGUMENT

For the Board's convenience, claims 1-23 are one group that will stand or fall together. As will be explained, the Final Office Action fails to meet the burden to establish non-obviousness based on the disparate references and as such the claims are allowable over the cited art of record.

A. The Combined Three References Relate To Vastly Different Technologies

The claims are directed toward efficient yet secure authentication for gaming machines. The Jackson and Pease references are representative of prior art authentication requiring the examination of all blocks in a memory volume. Such prior art schemes suffer from lack of fast authentication since all blocks must be authenticated in a particular memory volume. As will be discussed, the Burrows reference would not be considered in combination with the other references by one of ordinary skill in the art since Burrows does not relate to security and authentication.

Due to the need to comply with gaming regulations as well as the desire to insure that wagering games are not tampered with, gaming software is authenticated on a periodic basis and on the occurrence of certain events such as if a door is open in the cabinet, on reset or when the wagering game commences. Secure hashing is used to produce a unique representation (hash key-value) of the software and the unique representation is checked against a stored value to authenticate the software. In order to produce a sufficiently unique hash key-value, complex computational steps must be performed on the underlying data. However, the need for secure hashing for authentication is balanced by the desire to rapidly authenticate game software to minimize delays in allowing players to play the wagering game.

The present claims address both these concerns by calculating hash key-values from non-sequential data blocks based on random starting addresses. In this manner, the speed of authentication is enhanced because not every data block in a media is used in determining the hash key-value. However, security is insured because a sufficient amount of the data is verified by a unique hash key-value to meet security requirements.

Jackson is representative of commonly known prior art authentication that requires the hash based on all memory blocks and therefore authenticates every data block of a gaming software program during program operation. (Ex. D, ¶ 81). Jackson's authentication method, while meeting security requirements, takes time especially for larger game software programs, and therefore slows down wagering game operation because all blocks of memory must be authenticated. Further, Jackson starts at the first block of the memory devices and sequentially proceeds through each memory block to determine the hash key. (Ex. D, ¶ 88). The Final Office Action acknowledges that Jackson does not teach "setting an address pointer ADDR to a first next memory location in the device, setting the next ADDR to a next memory location in the device to be authenticated, and adding a predetermined number N to the ADDR such that a next $ADDR = ADDR + N$, and that N is equal to a positive or negative integer excluding -1, 0, and 1." (Ex. B, pp. 3-4).

Pease relates to a general method of authentication that uses unused memory 27 for part of the random-looking (but reproducible) data (termed non-sequential data) at boot time in the authentication calculations. (Ex. E, Fig. 2). Pease discloses using a non-associative technique in a circular way to verify the data, but does not always start at the data blocks in the beginning of the device in the verification process. (Ex. E, Col. 4, ll. 20-38). Pease also discloses authenticating every file in the device, thus resulting in a process that has adequate security but, as with prior art such as Jackson, requires excessive time and processor resources to authenticate every block in a memory device. (Ex. E, Col. 4, ll. 33-38).

Burrows is directed toward another technical problem unrelated to authentication, namely detection of spam e-mail. (Ex. F, Abstract). Present spam detection systems present an e-mail sender with a "puzzle" to send e-mail. An automatic "spam" generator cannot solve the "puzzle"

and therefore spam e-mail is thwarted. However, because different computers present the “puzzle” at different speeds, present spam filters result in undesirable delays for slower computers. (Ex. F, Col. 4, l. 63 to Col. 5, l. 3). Burrows relies on the fact that computer memory speeds (i.e., RAM memory speeds) are far less variable than CPU speeds. (Ex. F, Col. 5, ll. 6-19). Burrows relies on this computer feature to create a puzzle that can be solved in reasonable time by a variety of systems, all of which have a minimum amount of memory (larger than the largest processor cache), and therefore allow such systems to send non-spam e-mail messages. (Ex. F, Col. 5, ll. 14-19).

Burrows discloses the calculation of a checksum to rapidly match a received solution (X_0) to the “puzzle” to the acceptable solutions stored and not for an authentication function. (Ex. F, Col. 12, ll. 35-38). If the solution is stored, indicating a correct solution to the “puzzle,” the message may be sent. (Ex. F, Col. 12, ll. 34-38). Without the checksum, the puzzles generated may have multiple solution sets. (Ex. F, Col. 12, ll. 29-34). The checksum is used to disambiguate the multiple solution sets to arrive at the single solution that is expected as the solution of the “puzzle.” The checksum is calculated over a short sequence of values, which can be a subset of the sequence forming the puzzle solution. A subset of the path may be chosen because the checksum of the subset is sufficient to find the correct puzzle solution as there are only a few solutions within the solution sets. (Ex. F, Col. 12, ll. 38-40).

B. Claim 1 Is Allowable Over The Impermissibly Combined References

The Final Office Action combines Jackson, Pease and Burrows in the obviousness rejection against claim 1. Applicant respectfully submits that the combination of these references to achieve the claimed subject matter constitutes impermissible hindsight. The Final Office Action cites Jackson as the base reference. Because Jackson requires authentication of all

of the software on a media device, it suffers from the problems explained above and is an example of known authentication art. Claim 1 departs from the teaching of such art to achieve certain advantages noted above by requiring that the hash key-value be determined based on addresses (ADDR) of memory by “adding a predetermined number N to said ADDR such that a next ADDR=ADDR+N, wherein N is equal to a positive or negative integer excluding -1, 0 and 1.” In such a manner, only certain memory blocks are used to determine the hash key-value thus ensuring adequate security due to the hashing algorithm but increasing the speed of authentication. The Final Office Action then applies Pease and Burrows, two disparate references, to modify Jackson in order to render the remaining elements of claim 1 obvious. Applicant respectfully submits that this combination is improper as one of ordinary skill in the art would not apply Burrows to authentication needs outlined in Jackson and Pease.

1. There is No Suggestion To Make Authentication More Efficient In Either Jackson or Pease

There is no suggestion in either Pease or Jackson to shorten the authentication process and thus use a process based on selected blocks in a memory device as asserted by the Final Office Action. Evaluation of obviousness under *KSR* was outlined in the Federal Register dated October 10, 1007. (Vol. 72, No. 195). The *KSR* rationale presumably offered by the Final Office Action is Rationale G of the Federal Register, suggestion or motivation to combine. Rationale (G) Teaching, Suggestion or Motivation to Combine, requires the Examiner to articulate the following:

- 1) a finding that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings;
- 2) a finding that there was a reasonable expectation of success; and
- 3) whatever additional findings based on the *Graham* factual inquires may be necessary, in view of the facts of the case under consideration, to explain a conclusion of obviousness.

(Federal Register, p. 57534).

The Final Office Action has not provided any rationale for combining Burrows with authentication references such as Jackson and Pease given their different features. Neither Jackson nor Pease suggests or discloses that authentication should be made more efficient by running an authentication algorithm on less than all of a memory volume. In fact both references require the authentication of all files in a volume therefore teaching away from a more efficient, yet adequately secure authentication process.

2. Burrows Is Not In The Authentication Field and Would Not be Considered By One of Ordinary Skill In The Art To Improve Either Jackson or Pease

The Final Office Action suggests that one of ordinary skill would combine the checksum of Burrows, a spam filtering system, to authentication systems such as Jackson and Pease. As explained above, Burrows generally relates to designing a “puzzle” or problem that is easy to generate and hard to solve for a machine. (Ex. F, Col. 1, ll. 17-21). This is used for spam prevention, as a sender of a spam message will not devote the resources to solving a problem generated by Burrows’ functions but a sender of limited e-mails will have the necessary computer resources to solve the problem to send the e-mail, thus providing an indication that an e-mail message sent by the computer is not spam. (Ex. F, Col. 1, ll. 14-18). The section cited by the Final Office Action uses a checksum to rapidly match a received solution (X_0) to the “puzzle” to the acceptable solutions stored. (Ex. B, p. 4, Ex. F, Col. 12, ll. 35-41).

The checksum disclosed in Burrows is therefore directed to help rapidly search for an item (acceptable solution to a “puzzle”) but has no security function whatsoever. It is not necessary to calculate a checksum for all the solutions because it is unnecessary to determine an exact match. The checksum is designed to help narrow finding the correct solution to the

“puzzle” to match the offered solution and therefore send the e-mail. However, the checksum value in Burrows may be easily faked because it is not complex and not designed for a sufficiently unique representation of the solution data that is required for secure authentication.

In contrast, claim 1 requires “applying a hashing algorithm” which is a secure function that takes an input string (usually a string of digits) and converts (“hashes”) it to a fixed size, usually smaller, output string (“hash key-value”). The object of secure authentication is to “fingerprint” the input string so that the resulting hash key-value is very likely to represent one and only one input string for a data file. A hash key-value produced by a hashing algorithm has several properties that allow its application to secure authentication. For example, changing a single bit of the input string will result in a different hash key-value thus indicating tampering of the data.

The hashing algorithm is also a non-invertible function that prevents duplication of a unique hash for message. An invertible function, such as a checksum, allows the same value for different data. For example, if two blocks were switched, the checksum is the same, but the hash value would be different. This property is necessary for security because alterations in the underlying data such as changing the order of blocks or changing the underlying data may be detected in an alteration of the hash key-value. In fact, the secure properties of hashing algorithms allow the compliance with security-based governmental regulations for wagering game machines.

As simple mathematical functions such as checksums are easily subverted, they are not appropriate for effective security and are not considered as an adequate solution for secure functions such as authentication. One of ordinary skill in the art would recognize that: “these types of redundancy checks are useful in detecting *accidental* modification such as corruption to

stored data or errors in a communication channel. However, they provide no security against a malicious agent as their simple mathematical structure makes them trivial to circumvent.”

(<http://en.wikipedia.org/wiki/Checksum>). For example, a data set may be easily modified to produce the same checksum as a different data set. A checksum is thus insecure and could not be used for reliable verification of a unique set of data for the purpose of authentications.

Checksums clearly do not meet governmental regulations relating to proper authentication of wagering game machines.

A person of ordinary skill in the art would not reference Burrows if it were desired to make an authentication process as outlined in either Jackson or Burrows more efficient. First, Burrows does not deal with authentication (i.e., a proof of origin) or security issues and therefore is in different field of technology than that of the claims (or Jackson and Pease for that matter). The checksum in Burrows is really a shortened identifier such as a first name, used to distinguish the requested solution from a set of possible ones. Checksums are not designed for security functions and especially in the context of Burrows (use in simple search) would not be in the authentication art. Contrary to the assertion of the Final Office Action, one of ordinary skill in the art would not look to apply a checksum of a tree method for locating an object for the purpose of spam prevention in Burrows to an authentication problem as in the present claims.

Second, one of ordinary skill in the authentication field would not look to solutions relating to checksums because they are inherently insecure. As explained above, checksums are easily replicated for different sets of data thus providing no security function whatsoever. Particularly, in view of gaming applications, one of ordinary skill would not reference Burrows because a checksum could not meet applicable regulations governing wagering game machines.

The combination of Burrows with references requiring secure hashing such as Jackson or Pease is therefore improper and claim 1 is non-obvious over the cited references.

One of ordinary skill would not have any motivation to solve the problems that are outlined by the claims based on Pease or Jackson. Further one of ordinary skill would not look to Burrows in the field of spam detection for application to authentication. Therefore, the combination of Burrows to Pease and Jackson is unsupportable and claims 1-12 are allowable.

C. Claims 13 and 17 Are Allowable Over The Impermissibly Combined References

The Final Office Action uses similar rationales to reject claims 13 and 17 based on Jackson in combination with Pease and Burrows. (Ex. B, pp. 8-11). Both of these claims require that the hash calculation is performed from a sample of memory locations, the “sample of memory locations being a number of memory locations that is less than said plurality of memory locations and each memory location of said sample of memory locations is separated from other memory locations of said sample of memory locations by at least one memory location.” The Final Office Action concedes that Jackson “does not explicitly disclose memory locations in the form of addresses or the like, that the hash calculation is performed on a sample of memory locations being a number of memory locations that is less than all of the plurality of memory locations and that each memory location of the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory location.” (Ex. B, p. 8). The Final Office Action asserts that one of ordinary skill would incorporate the checksum techniques of Burrows into Jackson in order to increase the speed of the integrity checks. (Ex. B, pp. 9 and 11).

As explained above, one of ordinary skill in the art would not apply the techniques of Burrows to Jackson or any other security application because the references are in different

technical fields. Moreover, because of the unique requirements of secure authentication and verification, one of ordinary skill would not look to the field of searching to apply checksum techniques to a security method such as Jackson or Pease. Finally, the Final Office Action has not supplied any motivation or teaching from Jackson and Pease to sample less than all memory locations to provide the basis of the hash calculation. Claims 13 and 17 are therefore allowable because the combination of Burrows with Jackson and Pease is improper.

VIII. CLAIMS APPENDIX

A clean copy of the claims 1-23 involved in the appeal is included in the Claims Appendix.

IX. EVIDENCE APPENDIX

A copy of the evidence relied upon by the appellant is included in the Evidence Appendix and is herein referenced. A list of evidence and where each was entered in the record is included in the Index to the Appendices.

X. RELATED PROCEEDINGS APPENDIX

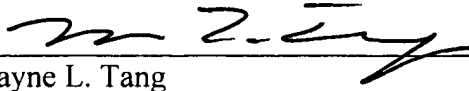
As there are no related proceedings, no information is provided in the Related Proceedings Appendix.

XI. CONCLUSION

For at least the foregoing reasons, the final rejection of appealed claims 1-23 set forth in the Final Office Action mailed February 28, 2008, should be reversed.

Respectfully submitted,

Date: August 5, 2008



Wayne L. Tang
Reg. No. 36,028
NIXON PEABODY, LLP.
161 N. Clark Street, 48th Floor
Chicago, Illinois 60601-3213
(312) 425-3900
Attorney for Applicants



INDEX TO THE APPENDICES

SUBJECT

EXHIBIT

CLAIM APPENDIX

EVIDENCE APPENDIX

LIST OF EVIDENCE

U.S. Publication No. 2005/014317	A
Final Office Action dated February 28, 2008	B
Notice of Appeal Filed June 5, 2008	C
U.S. Patent Publication No. 2002/0049909 ("Jackson")	D
U.S. Patent No. 5,644,704 ("Pease")	E
U.S. Patent No. 7,149,801 ("Burrows")	F

RELATED PROCEEDINGS APPENDIX



**CLAIMS APPENDIX
CLEAN COPY OF CLAIMS ON APPEAL**

1. In a gaming machine, a method of authenticating a media device comprising:
setting an address pointer ADDR to a first next memory location in said media device;
determining whether said first next memory location is a last memory location to be authenticated in said media device;
applying a hashing algorithm to contents of said first next memory location and updating a key-value;
adding a predetermined number N to said ADDR such that a next ADDR=ADDR+N, wherein N is equal to a positive or negative integer excluding -1, 0 and 1;
setting said next ADDR to a next memory location in the media device to be authenticated such that said next memory location is separated from said first next memory location by at least one memory location;
repeating the determining, applying, adding and setting steps until said next ADDR is equal to said last memory location;
determining whether said key-value is equal to a predetermined key;
in response to said key-value being equal to said predetermined key, passing authentication; and
in response to said key-value not being equal to said predetermined key, failing authentication.
2. The gaming machine utilizing the method of claim 1, wherein said first next memory location is a first memory location of said media device.
3. The gaming machine utilizing the method of claim 1, wherein said last memory location to which said next ADDR is equal is not the actual last memory location of said media device.
4. The gaming machine utilizing the method of claim 1, further comprising:
calculating a random number S, wherein S is an integer from 0 to N; and
adding S to N such that N=S+N prior to setting said address pointer ADDR to said first next memory location in said media device.

5. The gaming machine utilizing the method of claim 4, wherein said predetermined key is equal to $Z(S)$, such that $Z(S)$ is equal to one of S predetermined keys.

6. The gaming machine utilizing the method of claim 5, wherein $Z(S)$ is calculated and stored prior to a first time said gaming machine is authenticated.

7. The gaming machine utilizing the method of claim 1, wherein said predetermined key is calculated and stored prior to a first time said gaming machine is authenticated.

8. The gaming machine utilizing the method of claim 1, further comprising:
calculating said predetermined number N such that N is equal to a number from 1 to P ,
wherein P is less than a number of memory locations in said media device to be authenticated;
and

wherein said setting said address pointer $ADDR$ to said first next memory location in said media device comprises setting $ADDR$ to N .

9. The gaming machine utilizing the method of claim 8, wherein said predetermined key is equal $Z(P)$ such that $Z(P)$ is equal to one of P predetermined keys

10. The gaming machine utilizing the method of claim 9, wherein $Z(P)$ is calculated prior to a first authentication of said gaming machine.

11. The gaming machine utilizing the method of claim 1, wherein said hashing algorithm is a SHA-1 algorithm.

12. The gaming machine utilizing the method of claim 1 further comprising resetting said address pointer $ADDR$ to said first next memory location in said media device after passing authentication such that said method repeats continuously until said media devices fails authentication or said gaming device is turned off.

13. A gaming machine comprising:

a user interface; and
a central processing unit (CPU) coupled to said user interface, said CPU comprising:
a processor;
a first memory coupled to said processor, said first memory adaptable to store data in a plurality of memory locations;
a second memory coupled to said processor, said second memory adapted to contain executable program code, said executable program code further comprises a plurality of instructions configured to cause said processor to determine the authenticity of said data in said plurality of memory locations, said instructions include instructions for:
performing a hash calculation on a sample of memory locations from said plurality of memory locations and calculating a key-value from said sample of memory locations, said sample of memory locations being a number of memory locations that is less than said plurality of memory locations and each memory location of said sample of memory locations is separated from other memory locations of said sample of memory locations by at least one memory location;
comparing said key-value to a predetermined key;
authenticating said data stored in said plurality of memory locations if said key-value is equal to said predetermined key; and
not authenticating said data stored in said plurality of memory locations if said key-value is not equal to said predetermined key.

14. The gaming machine of claim 13 wherein each one of the memory locations in said sample of memory locations are separated by N memory locations, wherein N is equal to a positive or negative integer excluding -1, 0 and 1.

15. The gaming machine of claim 14, wherein said instructions further include instructions for selecting the number N from a random number less than the number of memory locations in said plurality of memory locations.

16. The gaming machine of claim 14, wherein the number of memory locations in said plurality of memory locations is equal to the total number of memory locations in said first memory.

17. In a gaming machine that is turned on, a method of repeatedly authenticating a portion of a media device, said method comprising:

reading a plurality of memory locations that are spaced from each other in said media device, such that each of said plurality of memory locations that is read is separated from the other memory locations by at least one memory location, said plurality of memory locations being less than a total number of memory locations in said media device;

after reading each memory location, calculating a hash value and using said hash value to update a key-value until all said plurality of memory locations are read and a final key-value is determined;

comparing said final key-value to a predetermined key;

passing said portion of said media device as authentic if said final key-value is equal to said predetermined key and repeating said reading, calculating and comparing steps; and

failing said predetermined portion of said media device as authentic if said final key-value is not equal to said predetermined key and halting operation of said gaming machine.

18. The method of claim 17, wherein said portion of said media device is equal to all the memory locations in said media device.

19. The method of claim 17, wherein said plurality of memory locations are equally spaced from each other.

20. The method of claim 17, wherein said plurality of memory locations are equally spaced from each other by a number N , such that N is randomly selected each time the step of reading is performed, N is equal to a number that is less than the total number of memory locations in said media device

21. The method of claim 20, wherein N is randomly selected from a number that is less than 20.

22. The method of claim 17, wherein said plurality of memory locations are equally spaced from each other and the first memory location read is a random number S from a first possible

memory location that can be read.

23. The method of claim 22, wherein S is recalculated prior to said reading step.

Evidence Appendix

Exhibit A



US 20050143171A1

(19) **United States**(12) **Patent Application Publication** (10) **Pub. No.: US 2005/0143171 A1**
Loose (43) **Pub. Date: Jun. 30, 2005**(54) **GAMING MACHINE HAVING SAMPLED
SOFTWARE VERIFICATION****Publication Classification**(76) **Inventor: Timothy C. Loose, Chicago, IL (US)**(51) **Int. Cl.⁷ G06F 17/00; G06F 19/00**(52) **U.S. Cl. 463/29**

Correspondence Address:
JENKENS & GILCHRIST, P.C.
225 WEST WASHINGTON
SUITE 2600
CHICAGO, IL 60606 (US)

(57) **ABSTRACT**

A gaming machine adapted to authenticate the contents of a media device (memory device) by sampling a number of memory locations in the media device. A hash function is applied to the contents of the sampled memory locations thereby calculating a key-value. The key-value is compared to a previously calculated key. If the key-value and the key are equal, then the media device is considered authentic.

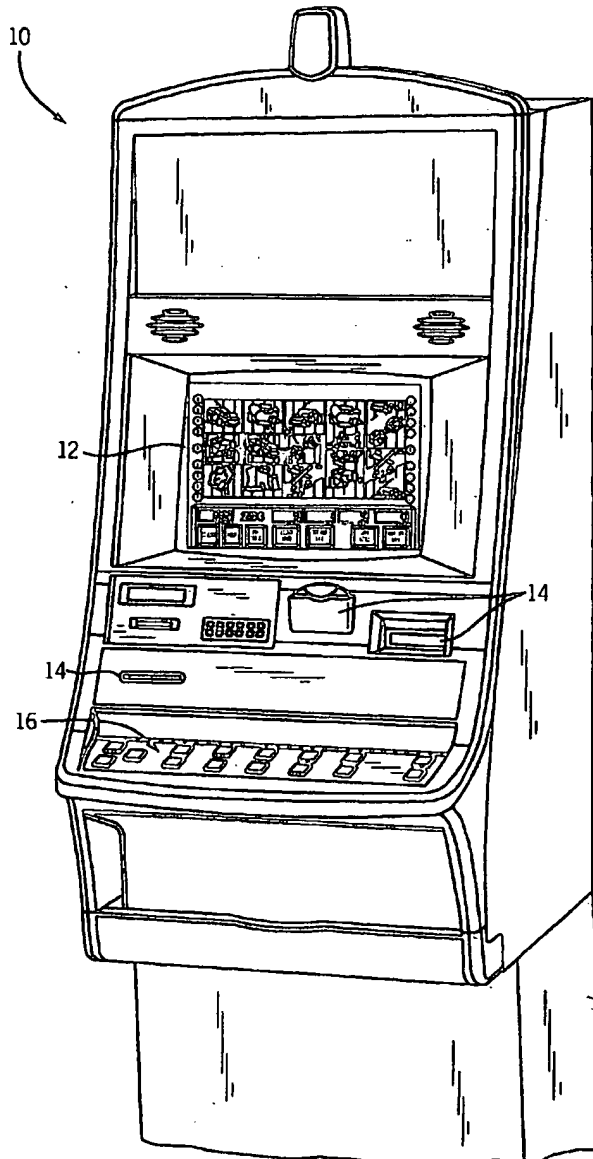
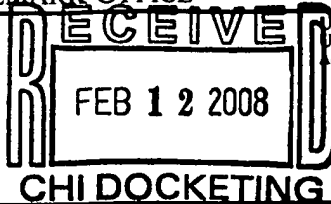
(21) **Appl. No.: 10/748,489**(22) **Filed: Dec. 30, 2003**

Exhibit B



UNITED STATES PATENT AND TRADEMARK OFFICE



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/748,489

12/30/2003

Timothy C. Loose

47079-00243USPT

8735

30223 7590 02/08/2008
NIXON PEABODY LLP
161 N. CLARK STREET
48TH FLOOR
CHICAGO, IL 60601-3213

EXAMINER

POPHAM, JEFFREY D

DOCKETED

ART UNIT

PAPER NUMBER

2137

INIT. U DATE: 2/12/08
Open
ACTION due DATE: 4/8/08
DL 8/8/08

MAIL DATE

DELIVERY MODE

02/08/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/748,489

Applicant(s)

LOOSE, TIMOTHY C.

Examiner

Jeffrey D. Popham

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Remarks

Claims 1-23 are pending.

Response to Arguments

1. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-7, 11-14, 16-19, 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson (U.S. Patent Application Publication 2002/0049909) in view of Pease (U.S. Patent 5,644,704) and Burrows (U.S. Patent 7,149,801).

Regarding Claim 1,

Jackson discloses in a gaming machine, a method of authenticating
a media device comprising:

Determining a first next memory location in the media device

(Paragraph 81 and 87-89);

Determining whether the first next memory location is a last memory location to be authenticated in the media device (Paragraph 81 and 87-89);

Applying a hashing algorithm to contents of the first next memory location and updating a key value (Paragraph 81 and 87-89);

Determining a next memory location in the media device to be authenticated such that the next memory location is separated from the first next memory location by at least one memory location (Paragraph 81 and 87-89);

Repeating the determining, applying, adding, and setting steps until the next memory location is equal to the last memory location (Paragraph 81 and 87-89);

Determining whether the key value is equal to a predetermined key (Paragraph 81 and 87-89);

In response to the key value being equal to the predetermined key, passing authentication (Paragraph 81 and 87-89); and

In response to the key value not being equal to the predetermined key, failing authentication (Paragraph 81 and 87-89);

But does not explicitly disclose setting an address pointer ADDR to a first next memory location in the device, setting the next ADDR to a next memory location in the device to be authenticated, and adding a predetermined number N to the ADDR such that a next ADDR = ADDR +

Art Unit: 2137

N, and that N is equal to a positive or negative integer excluding -1, 0, and 1.

Pease, however, discloses memory locations in the form of addresses, setting an address pointer ADDR to a first next memory location in the device, setting the next ADDR to a next memory location in the device to be authenticated, and adding a predetermined number N to the ADDR such that a next ADDR = ADDR + N (Column 2, lines 14-33; and Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that N is equal to a positive or negative integer excluding -1, 0, and 1 (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 2,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the first next memory location is a first memory location of the media device (Paragraph 81 and 87-89); and Pease discloses that the first next memory location is a first memory location of the media device (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 3,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Pease discloses that the last memory location to which the next ADDR is equal is not the actual last memory location of the media device (Column 4, lines 20-37).

Regarding Claim 4,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Pease discloses calculating a random number S , wherein S is an integer from 0 to N and adding S and N prior to setting the address pointer ADDR to said first next memory location in the media device (Column 2, lines 14-33; and Column 3, lines 26-65); and Burrows discloses adding S to N such that $N = S + N$ (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 5,

Jackson as modified by Pease and Burrows discloses the method of claim 4, in addition, Jackson discloses that the predetermined key is

Art Unit: 2137

equal to $Z(S)$, such that $Z(S)$ is equal to one of S predetermined keys (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is equal to $Z(S)$, such that $Z(S)$ is equal to one of S predetermined keys (Column 4, line 54 to Column 5, line 3).

Regarding Claim 6,

Jackson as modified by Pease and Burrows discloses the method of claim 5, in addition, Jackson discloses that $Z(S)$ is calculated prior to a first time the device is authenticated (Paragraphs 81 and 87-89); and Pease discloses that $Z(S)$ is calculated prior to a first time the device is authenticated (Column 4, line 54 to Column 5, line 3).

Regarding Claim 7,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the predetermined key is calculated and stored prior to a first time the media device is authenticated (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is calculated and stored prior to a first time the media device is authenticated (Column 4, line 54 to Column 5, line 3).

Regarding Claim 11,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses that the hashing algorithm is a SHA1 algorithm (Paragraphs 81 and 87-89).

Regarding Claim 12,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Jackson discloses resetting the authentication process in the media device after passing authentication such that the method repeats continuously until the media device fails authentication or the gaming device is turned off (Paragraphs 81, 85, and 87-89); and Pease discloses setting the address pointer ADDR to the first next memory location (Column 2, lines 14-33; and Column 3, lines 26-65)

Regarding Claim 13,

Jackson discloses a gaming machine comprising:

A user interface (Paragraph 48); and

A CPU coupled to the user interface (Paragraphs 53-54), the CPU comprising:

A processor (Paragraphs 53-54);

A first memory coupled to the processor, the first memory adaptable to store data in a plurality of memory locations (Paragraphs 53-54);

A second memory coupled to the processor, the second memory adapted to contain executable program code, the executable program code further comprises a plurality of instructions configured to cause the processor to determine the authenticity of the data in the plurality of memory locations (Paragraphs 53-58), the instructions include instructions for:

Performing a hash calculation on data of memory locations from the plurality of memory locations and calculating a key value from the data of memory locations (Paragraph 81 and 87-89);

Comparing the key value to a predetermined key (Paragraph 81 and 87-89);

Authenticating the data stored in the plurality of memory locations if the key value is equal to the predetermined key (Paragraph 81 and 87-89); and

Not authenticating the data stored in the plurality of memory locations if the key value is not equal to the predetermined key (Paragraph 81 and 87-89);

But does not explicitly disclose memory locations in the form of addresses or the like, that the hash calculation is performed on a sample of memory locations being a number of memory locations that is less than all of the plurality of memory locations and that each memory location of the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory locations.

Pease, however, discloses memory locations in the form of addresses (Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory

Art Unit: 2137

to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that the sample of memory locations are a number of memory locations that is less than all of the plurality of memory locations and each memory location of the sample of memory locations is separated from other memory locations of the sample of memory locations by at least one memory location (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 14,

Jackson as modified by Pease and Burrows discloses the machine of claim 13, in addition, Burrows discloses that each one of the memory locations in the sample of memory locations are separated by N memory locations, wherein N is equal to a positive or negative integer excluding -1, 0, and 1 (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 16,

Jackson as modified by Pease and Burrows discloses the machine of claim 13, in addition, Pease discloses that the number of memory

locations in the plurality of memory locations is equal to the total number of memory locations in the first memory (Column 3, lines 26-65).

Regarding Claim 17,

Jackson discloses in a gaming machine that is turned on, a method of repeatedly authenticating a portion of a media device, the method comprising:

Reading a plurality of memory locations that are spaced from each other in the media device (Paragraph 81 and 87-89);

After reading each memory location, calculating a hash value and using the hash value to update a key value until all of the plurality of memory locations are read and a final key value is determined (Paragraph 81 and 87-89);

Comparing the final key value to a predetermined key (Paragraph 81 and 87-89);

Passing the portion of the media device as authentic if the final key value is equal to the predetermined key and repeating the reading, calculating and comparing steps (Paragraph 81 and 87-89); and

Failing the portion of the media device as authentic if the final key value is not equal to the predetermined key and halting operating of the gaming machine (Paragraph 81 and 87-89);

But does not explicitly disclose memory locations in the form of addresses or the like, and that each of the plurality of memory locations

Art Unit: 2137

that is read is separated from the other memory locations by at least one memory location, the plurality of memory locations being less than a total number of memory locations in the media device.

Pease, however, discloses memory locations in the form of addresses (Column 3, lines 26-65). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the data addressing and verification system of Pease into the secure gaming system of Jackson in order to allow authentication of data/memory to begin at any starting address and proceed through used as well as unused portions of memory, thereby providing a better verification or authentication of memory.

Burrows, however, discloses that each of the plurality of memory locations that is read is separated from the other memory locations by at least one memory location, the plurality of memory locations being less than a total number of memory locations in the media device (Column 8, lines 54-60; and Column 12, lines 35-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the checksum techniques of Burrows into the secure gaming system of Jackson as modified by Pease in order to increase the speed with which the system can perform integrity checks.

Regarding Claim 18,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Pease discloses that the portion of the media device is equal to all the memory locations in the media device (Column 3, lines 26-65).

Regarding Claim 19,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other (Column 8, lines 54-60; and Column 12, lines 35-41).

Regarding Claim 22,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other (Column 8, lines 54-60; and Column 12, lines 35-41); and Pease discloses that the first memory location read is a random number S from a first possible memory location that can be read (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 23,

Jackson as modified by Pease and Burrows discloses the method of claim 22, in addition, Pease discloses that S is recalculated prior to the reading step (Column 2, lines 14-33; and Column 3, lines 26-65).

Art Unit: 2137

3. Claims 8-10, 15, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jackson in view of Pease and Burrows, further in view of Branstad (U.S. Patent 6,842,860).

Regarding Claim 8,

Jackson as modified by Pease and Burrows discloses the method of claim 1, in addition, Burrows discloses choosing a predetermined number N such that N is equal to a number from 1 to P, wherein P is less than a number of memory locations in the device to be authenticated (Column 8, lines 54-60; and Column 12, lines 35-41); and Pease discloses that setting the address pointer ADDR to the first next memory location in the media device comprises setting ADDR to N (Column 2, lines 14-33; and Column 3, lines 26-65); but may not explicitly disclose calculating the predetermined number N.

Branstad, however, discloses calculating a predetermined number N being a number from 1 to P, wherein P is less than a number of memory locations in the device to be authenticated (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be

used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 9,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 8, in addition, Jackson discloses that the predetermined key is equal to $Z(P)$ such that $Z(P)$ is equal to one of P predetermined keys (Paragraphs 81 and 87-89); and Pease discloses that the predetermined key is equal to $Z(P)$ such that $Z(P)$ is equal to one of P predetermined keys (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 10,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 9, in addition, Jackson discloses that $Z(P)$ is calculated prior to a first authentication of the media device (Paragraphs 81 and 87-89); and Pease discloses that $Z(P)$ is calculated prior to a first authentication of the media device (Column 2, lines 14-33; and Column 3, lines 26-65).

Regarding Claim 15,

Jackson as modified by Pease and Burrows does not explicitly disclose that the instructions further include instructions for selecting the number N from a random number less than the number of memory locations in the plurality of memory locations.

Branstad, however, discloses that the instructions further include instructions for selecting the number N from a random number less than the number of memory locations in the plurality of memory locations (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 20,

Jackson as modified by Pease and Burrows discloses the method of claim 17, in addition, Burrows discloses that the plurality of memory locations are equally spaced from each other by a number N, such that N is equal to a number that is less than the total number of memory locations in the media device (Column 8, lines 54-60; and Column 12, lines 35-41); but does not explicitly disclose that N is randomly selected each time the step of reading is performed.

Branstad, however, discloses that N is randomly selected each time the step of reading is performed (Column 19, lines 26-55). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the partial message authentication code

Art Unit: 2137

techniques of Branstad into the secure gaming system of Jackson as modified by Pease and Burrows in order to provide for additional randomness in the determination of which memory locations are to be used in computation of the key value, thereby making it harder for a malicious entity to modify data without being detected.

Regarding Claim 21,

Jackson as modified by Pease, Burrows, and Branstad discloses the method of claim 20, in addition, Branstad discloses that N is randomly selected from a number (Column 19, lines 26-55); and Burrows discloses that such number can be less than 20 (Column 12, lines 35-41).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2137

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Jeffrey D Popham
Examiner
Art Unit 2137

JP

2,7108

Notice of References Cited

Application/Control No.

10/748,489

Applicant(s)/Patent Under

Reexamination

LOOSE, TIMOTHY C.

Examiner

Jeffrey D. Popham

Art Unit

2137

Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,644,704 A	07-1997	Pease et al.	714/42
*	B	US-7,149,801 B2	12-2006	Burrows et al.	709/225
*	C	US-6,842,860 B1	01-2005	Branstad et al.	713/170
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Exhibit C

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES	Docket Number (Optional) 247079-00243USPT
--	---

	In re Application of Timothy C. Loose	
	Application Number 10/748,489	Filed December 30, 2003
	For GAMING MACHINE HAVING SAMPLED SOFTWARE VERIFICATION	
	Art Unit 2137	Examiner Jeffrey D. Popham

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) \$ 510.00

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: \$ _____

☒ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-4181. I have enclosed a duplicate copy of this sheet.

☐ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

I am the

☐ applicant /inventor.

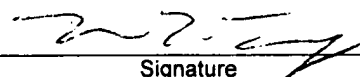
☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b)
is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.

Registration number 36,028

☐ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34. _____


Signature

Wayne L. Tang
Typed or printed name

(312) 425-8513
Telephone number

June 5, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

<input type="checkbox"/> *Total of <u>1</u> forms are submitted.
--

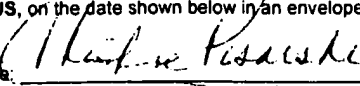
I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EM 143187610 US, on the date shown below in an envelope addressed to: MS AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.	
Dated: June 5, 2008	Signature:  (Christine Pisarski)

Exhibit D



US 20020049909A1

(19) **United States**(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0049909 A1****Jackson et al.**(43) **Pub. Date: Apr. 25, 2002**(54) **ENCRYPTION IN A SECURE
COMPUTERIZED GAMING SYSTEM**(30) **Foreign Application Priority Data**

Mar. 8, 2001 (US)..... PCT/US01/07381

(75) **Inventors: Mark D. Jackson, Fort Collins, CO
(US); Michael G. Martinek, Fort
Collins, CO (US)****Publication Classification**(51) **Int. Cl.⁷ G06F 12/14; H04L 9/32**(52) **U.S. Cl. 713/188; 713/189; 380/251**

Correspondence Address:

MARK A. LITMAN & ASSOCIATES, P.A.**York Business Center****Suite 205****3209 W. 76th St.****Edina, MN 55402 (US)**(57) **ABSTRACT**

The present invention provides an architecture and method for a gaming-specific platform that features secure storage and verification of game code and other data, provides the ability to securely exchange data with a computerized wagering gaming system, and does so in a manner that is straightforward and easy to manage. Some embodiments of the invention provide the ability to identify game program code as certified or approved, such as by the Nevada Gaming Regulations Commission or other regulatory agency. The invention provides these and other functions by use of encryption, including digital signatures and hash functions as well as other encryption methods.

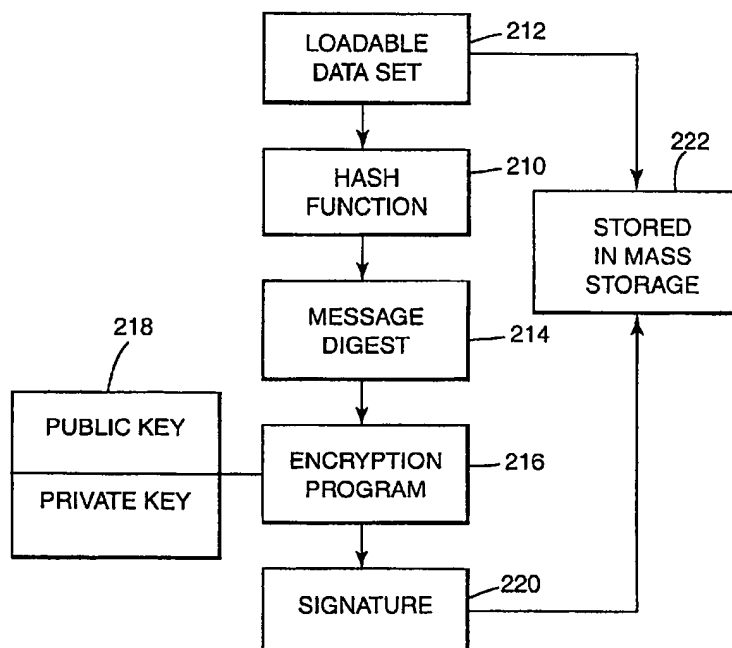
(73) **Assignee: Shuffle Master**(21) **Appl. No.: 09/949,021**(22) **Filed: Sep. 7, 2001****Related U.S. Application Data**(63) **Continuation-in-part of application No. 09/520,404,
filed on Mar. 8, 2000.**

Exhibit E

United States Patent [19]

Pease et al.

[11] Patent Number: 5,644,704

[45] Date of Patent: Jul. 1, 1997

[54] METHOD AND APPARATUS FOR
VERIFYING THE CONTENTS OF A
STORAGE DEVICE

[75] Inventors: Logan L. Pease, Reno; Delbert
Richard, Sparks; Peter D. Dickinson,
deceased, late of Reno, all of Nev., by
Kathy E. Dickinson, executrix

[73] Assignee: International Game Technology, Reno,
Nev.

[21] Appl. No.: 348,268

[22] Filed: Nov. 30, 1994

[51] Int. Cl.⁶ G06F 11/34

[52] U.S. Cl. 395/183.18; 371/21.5;
395/421.08; 395/183.16

[58] Field of Search 395/183.18, 183.16,
395/183.01, 185.01, 185.07, 421.08; 371/21.1,
21.5, 37.7

[56] References Cited

U.S. PATENT DOCUMENTS

3,825,905	7/1974	Allen, Jr.	395/200.19
3,838,264	9/1974	Maker	371/21.5
4,354,251	10/1982	Hellwig et al.	371/21.5
4,727,544	2/1988	Brunner et al.	371/21.5 X
5,488,702	1/1996	Byers et al.	395/186

OTHER PUBLICATIONS

Crenshaw, Jack W. Jan. 1992 Implementing CRCs.
Unknown 1968/1972 Error Control.

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Ly V. Hua

[57] ABSTRACT

A method and apparatus for verifying the contents of a storage device. A number of steps are involved in performing the verification. First, non-sequential data is written into each unused memory location of the storage device. Then, a non-associative technique is performed on contents of each memory location in the storage device starting at a randomly determined address in the storage device. Next, a final value from the non-associative technique is provided to a confirmation device for comparison with a set of predetermined resulting values. Then, the final value is compared to a resulting value, the resulting value being predetermined by applying the non-associative technique to pre-programmed contents of the storage device. Finally, one of two signals is generated. A first signal is generated indicating that the contents of the storage device are corrupted if the final value does not correspond to the resulting value. Alternatively, a second signal is generated indicating the contents of the storage device are uncorrupted if the final value corresponds to the resulting value.

21 Claims, 3 Drawing Sheets

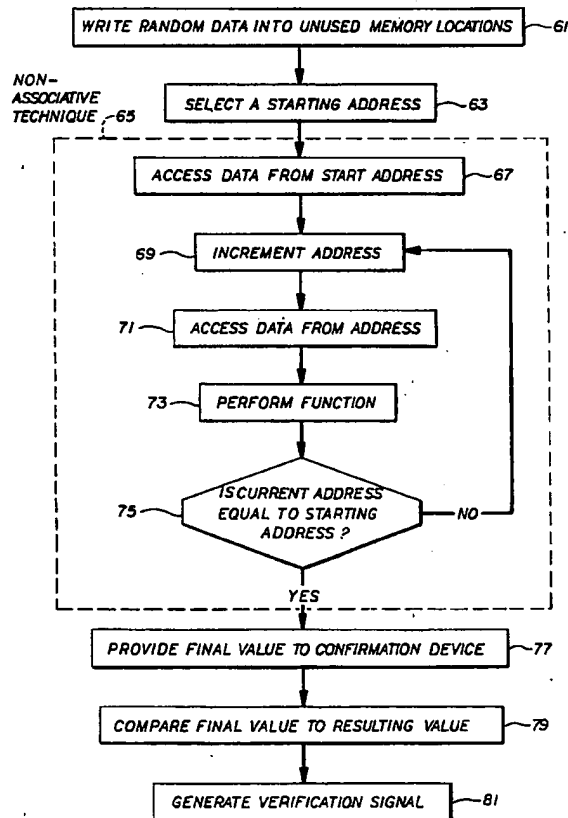


Exhibit F



US007149801B2

(12) United States Patent
Burrows et al.**(10) Patent No.: US 7,149,801 B2**
(45) Date of Patent: Dec. 12, 2006**(54) MEMORY BOUND FUNCTIONS FOR SPAM
DETERRENCE AND THE LIKE****(75) Inventors:** Michael Burrows, Palo Alto, CA (US);
Martin Abadi, Palo Alto, CA (US);
Mark Steven Manasse, San Francisco,
CA (US); Edward P. Wobber, Menlo
Park, CA (US); Daniel Ron Simon,
Redmond, WA (US)**(73) Assignee:** Microsoft Corporation, Redmond, WA
(US)**(*) Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 780 days.**(21) Appl. No.:** 10/290,879**(22) Filed:** Nov. 8, 2002**(65) Prior Publication Data**
US 2004/0093371 A1 May 13, 2004**(51) Int. Cl.**
G06F 15/173 (2006.01)
H04K 1/00 (2006.01)**(52) U.S. Cl.** 709/225; 713/201; 380/28**(58) Field of Classification Search** None
See application file for complete search history.**(56) References Cited****U.S. PATENT DOCUMENTS**

5,432,852 A *	7/1995	Leighton et al.	380/30
6,161,130 A	12/2000	Horvitz et al.	709/206
6,192,114 B1	2/2001	Council	379/114
6,662,300 B1 *	12/2003	Peters	713/182
2002/0120853 A1 *	8/2002	Tyree	713/188
2003/0044003 A1 *	3/2003	Chari et al.	380/28
2003/0172159 A1 *	9/2003	Schuba et al.	709/225
2004/0003283 A1 *	1/2004	Goodman et al.	713/201

2004/0030932 A1 *	2/2004	Juels et al.	713/202
2004/0059951 A1 *	3/2004	Pinkas et al.	713/202
2004/0068668 A1 *	4/2004	Lor et al.	713/201

OTHER PUBLICATIONSHashCash, <http://cypherspace.org/~adam/hashcash/>, Aug. 13, 2002, 4 pages.Camran, <http://www.camram.org/>, Aug. 13, 2002, 5 pages.Juels, A. et al., "Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks," *Proceedings of NDSS '99 (Networks and Distributed Security Systems)*, 1999, 151-165 and an abstract (1 page).

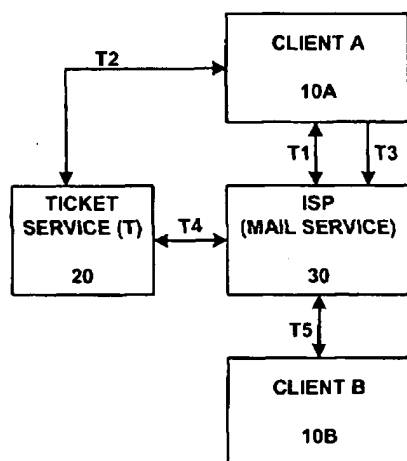
The CAPTCHA Project, "Telling Humans and Computers Apart (Automatically)," Aug. 13, 2002, 1 page.

Glassman, S. et al., "The Millicent Protocol for Inexpensive Electronic Commerce," *Fourth International World Wide Web Conference ("The Web Revolution")*, Boston, Massachusetts, Dec. 11-14, 1995, 21 pages.

(Continued)

Primary Examiner—Wen-Tai Lin**(74) Attorney, Agent, or Firm**—Woodcock Washburn LLP**(57) ABSTRACT**

A resource may be abused if its users incur little or no cost. For example, e-mail abuse is rampant because sending an e-mail has negligible cost for the sender. Such abuse may be discouraged by introducing an artificial cost in the form of a moderately expensive computation. Thus, the sender of an e-mail might be required to pay by computing for a few seconds before the e-mail is accepted. Unfortunately, because of sharp disparities across computer systems, this approach may be ineffective against malicious users with high-end systems, prohibitively slow for legitimate users with low-end systems, or both. Starting from this observation, we identify moderately hard, memory bound functions that most recent computer systems will evaluate at about the same speed, and we explain how to use them for protecting against abuses.

36 Claims, 6 Drawing Sheets**T1) A → ISP: REQUEST DELIVERY OF EMAIL TO B**
ISP → A: BOUNCE (W/ REF. TO T)**T2) A → T: REQUEST TICKET**
T → A: CHALLENGE & TICKET KIT**T3) A → ISP: TRANSMIT TICKET****T4) ISP → T: CANCEL TICKET**
T → ISP: OK**T5) ISP → B: DEPOSIT EMAIL FROM A INTO B'S
INBOX**

RELATED PROCEEDINGS APPENDIX

None. There are no related proceedings